

NETWORK ADDRESS CONVERSION METHOD AND ITS SYSTEM

Patent Number: JP2000059430
Publication date: 2000-02-25 ✓
Inventor(s): MARIO CARDONA ✓
Applicant(s):: MATSUSHITA ELECTRIC WORKS LTD ✓
Requested Patent: JP2000059430 (JP00059430)
Application Number: JP19980224454 19980807 ✓
Priority Number(s):
IPC Classification: H04L12/56 ; G06F13/00 ; H04L12/28 ; H04L12/66
EC Classification:
Equivalents: ✓

Abstract

PROBLEM TO BE SOLVED: To use in common a global Internet protocol IP address among a plurality of terminals configuring a private network at the same time, without converting a port number.

SOLUTION: Private hosts PH1, etc., stores a cross reference between a couple (PP, IA) of a port number PP given to a series of transaction processing and a global IP address IA internet hosts IH1, etc., and a private IP address PA to the internal table of an address converter AD. The global IP address GP is mapped onto private IP addresses PA of a plurality of private hosts PH1,etc., in terms of one to multi based on the cross reference. Since the port number PP and a packet port number GP are always in matching with each other, destruction of communication with an unknown host protocol is restrained to minimum, complications of the system are reclined and moreover the performance is improved.

Data supplied from the esp@cenet database - I2

3.

CP-860 US

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-59430

(P2000-59430A)

(43)公開日 平成12年2月25日 (2000.2.25)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 04 L 12/56		H 04 L 11/20	1 0 2 D
G 06 F 13/00	3 5 1	G 06 F 13/00	3 5 1 A
H 04 L 12/28		H 04 L 11/00	3 1 0 D
12/66		11/20	B

審査請求 未請求 請求項の数 5 OL (全 19 頁)

(21)出願番号 特願平10-224454

(22)出願日 平成10年8月7日(1998.8.7)

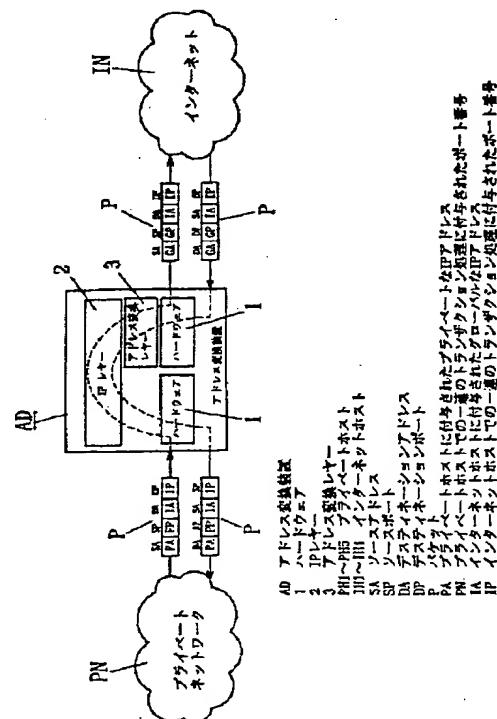
(71)出願人 000005832
松下電工株式会社
大阪府門真市大字門真1048番地(72)発明者 マリオ カルドナ
大阪府門真市大字門真1048番地松下電工株
式会社内(74)代理人 100087767
弁理士 西川 恵清 (外1名)

(54)【発明の名称】 ネットワークアドレス変換方法及びその装置

(57)【要約】

【課題】ポート番号を変換せずにプライベートなネットワークを構成する複数の端末間でグローバルなIPアドレスを同時に共有することを可能とする。

【解決手段】プライベートホストPH1…で一連のトランザクション処理に付与されたポート番号PP及びインターネットホストIH1…のグローバルIPアドレスIAの対(PP, IA)と、プライベートIPアドレスPAとの対応関係をアドレス変換装置ADの内部テーブルTaに記憶する。この対応関係に基づいて、1つのグローバルIPアドレスGPを複数台のプライベートホストPH1…のプライベートIPアドレスPAに1対多にマップすることができる。上記ポート番号PPとパケットのポート番号GPとが常に一致しているため、未知の上位プロトコルの通信を破壊するようなことを最小限に抑えることができ、システムの複雑さを減らし、且つ性能を向上させることができるとなる。



【特許請求の範囲】

【請求項1】 インターネットプロトコルにおけるプライベートなIPアドレスが付与された複数の端末から構成されるプライベートネットワークをインターネットに接続し、パケット毎にプライベートなIPアドレスと前記プライベートネットワークに付与されたグローバルなIPアドレスとのアドレス変換を行うアドレス変換手段によって前記各端末からインターネットへのパケットの送受信を可能とするネットワークアドレス変換方法において、前記アドレス変換手段にて前記各端末で一連のトランザクション処理に付与されたポート番号とパケットの送信先のグローバルなIPアドレスとの対を各端末のプライベートなIPアドレスに適宜対応付けることによってプライベートなIPアドレスとグローバルなIPアドレスとのアドレス変換を行うことを特徴とするネットワークアドレス変換方法。

【請求項2】 前記アドレス変換手段が備える内部テーブルに各端末での一連のトランザクション処理に付与されたポート番号及び送信先のグローバルなIPアドレスの対とプライベートなIPアドレスとの対応関係を記憶させ、プライベートネットワークから受信したパケットの送信元のポート番号及び送信先のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には前記内部テーブルに当該対と送信元のプライベートなIPアドレスとの対応関係を記憶するとともにパケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、一致する場合には当該パケットの送信元のプライベートなIPアドレスを前記内部テーブルの一一致した対応関係のプライベートなIPアドレスと比較して一致しない場合には当該パケットを廃棄するとともに一致する場合には当該パケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、インターネットから受信したパケットの送信先のポート番号及び送信元のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には当該パケットを廃棄するとともに、一致する場合には前記対応関係に基づいて当該パケットの送信先のアドレスをプライベートなIPアドレスに置き換えることを特徴とする請求項1記載のネットワークアドレス変換方法。

【請求項3】 インターネットプロトコルにおけるプライベートなIPアドレスが付与された複数の端末から構成されるプライベートネットワークをインターネットに接続し、パケット毎にプライベートなIPアドレスと前記プライベートネットワークに付与されたグローバルなIPアドレスとのアドレス変換を行って前記各端末からインターネットへのパケットの送受信を可能とするネットワークアドレス変換装置において、前記各端末で一連

のトランザクション処理に付与されたポート番号とパケットの送信先のグローバルなIPアドレスとの対を各端末のプライベートなIPアドレスに適宜対応付けることによってプライベートなIPアドレスとグローバルなIPアドレスとのアドレス変換を行うアドレス変換手段を備えたことを特徴とするネットワークアドレス変換装置。

【請求項4】 前記アドレス変換手段に各端末での一連のトランザクション処理に付与されたポート番号及び送信先のグローバルなIPアドレスの対とプライベートなIPアドレスとの対応関係を記憶する内部テーブルを備え、プライベートネットワークから受信したパケットの送信元のポート番号及び送信先のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には前記内部テーブルに当該対と送信元のプライベートなIPアドレスとの対応関係を記憶するとともにパケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、一致する場合には当該パケットの送信元のプライベートなIPアドレスを前記内部テーブルの一一致した対応関係のプライベートなIPアドレスと比較して一致しない場合には当該パケットを廃棄するとともに一致する場合には当該パケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、インターネットから受信したパケットの送信先のポート番号及び送信元のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には当該パケットを廃棄するとともに、一致する場合には前記対応関係に基づいて当該パケットの送信先のアドレスをプライベートなIPアドレスに置き換えることを特徴とする請求項3記載のネットワークアドレス変換装置。

【請求項5】 インターネットプロトコルにおけるルーティングやフィルタリングを行うルータの機能を備えたことを特徴とする請求項3又は4記載のネットワークアドレス変換装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、複数の端末で構成されるプライベートなネットワークからインターネットへパケットを送受信する際に、各端末のプライベートなIPアドレスをインターネットのグローバルなIPアドレスに変換するネットワークアドレス変換方法及びその装置に関するものである。

【0002】

【従来の技術】 近年、TCP/IP及びUDP/IPプロトコルをベースとしたインターネットの普及に伴い、IPアドレスの枯渇が重大な問題の一つになっている。この問題を解決する方法としては、アドレス変換によっ

てIPアドレスを共有するという方法がある。すなわち、インターネットで有効でないIPアドレス（プライベートIPアドレス）が付与された端末、例えばホストコンピュータ（以下、単に「ホスト」という）がインターネットで有効なIPアドレス（グローバルIPアドレス）を共有するのである。このようにアドレスを共有するためのアドレス変換方法としては、NAT（Network Address Translation RFC1631参照）と、

それに改良を加えたIPマスカレードという2つの方式が提唱されている。前者は、複数の端末（ホスト）が順次に、グローバルIPアドレスを共有することを可能とするものであり、後者は、複数の端末（ホスト）が同時にグローバルIPアドレスを共有することを可能とするものである。

【0003】ここで、図9に示すようにプライベートネットワークPNを構成する複数のホストPH1～PH5がアドレス変換装置AD”を介してインターネットINに接続されている場合を例にNAT及びIPマスカレードについてもう少し具体的に説明する。何れの方式においても共有されるのはプライベートネットワークPNに付与されているグローバルIPアドレス（アドレス変換装置AD”のインターネットIN側のIPアドレス）であり、共有を実施するのがアドレス変換装置AD”である。

【0004】まずNATにおいては、アドレス変換装置AD”がプライベートネットワークPNから受信したパケットを図10に示すフローチャートに従って処理するとともに、インターネットINから受信したパケットを図11に示すフローチャートに従って処理する。

【0005】図10に示すようにアドレス変換装置AD”はプライベートネットワークPNの任意のホスト（以下、「プライベートホスト」という）PH1…から受信したパケットの送信元のアドレス（プライベートホストPH1…に付与されているプライベートIPアドレス（以下、「PA」と表記）を読み出し（Step1）、現在アドレス変換装置AD”のグローバルIPアドレス（以下、「GA」と表記）に対応しているプライベートIPアドレスと一致するか否かを判断し（Step2）、一致しない場合にはそのパケットを廃棄し（Step5）、一致する場合にはパケット内のPAを格納する各フィールドにアドレス変換装置AD”のGAを書き込むことにより（Step3）、グローバルIPアドレスが付与されていないプライベートホストPH1…からのパケットの送信元アドレスをGAに変換する。そして、アドレス変換されたパケットをインターネットINに転送する（Step4）。

【0006】一方、アドレス変換装置AD”がインターネットINの任意のホストコンピュータ（以下、「インターネットホスト」という）IH1…からのパケットを受信すると、図11に示すようにパケット内のGAを格

納する各フィールドにGAに対応しているPAを書き込むことにより（Step1）、送信先のアドレスをアドレス変換装置AD”のGAから何れかのプライベートホストPH1…のプライベートIPアドレスに変換するアドレス変換を行い、アドレス変換されたパケットをプライベートネットワークPNに送る（Step2）。

【0007】而して、NATではアドレス変換装置AD”が自己のGAを何れか1台のプライベートホストPH1…のPAに一対一に対応させてアドレス変換を行っており、同時にインターネットINと接続可能なプライベートホストPH1…の台数が1台に限定されることになる。なお、パケットにはプライベートホストPH1…での一連のトランザクション処理に付与されるポート番号（以下、「PP」と表記）と、アドレス変換装置AD”からインターネットIN側に送受信されるパケットのポート番号（以下、「GP」と表記する）とは常に一致している（GP=PP）。

【0008】次にIPマスカレードにおいては、アドレス変換装置AD”が各プライベートホストPH1…のPAとプライベートホストPH1…でのトランザクション処理に付与されたポート番号PPの対（PA, PP）をユニークなポート番号GPに一対一に対応させ、その対応関係を内部テーブルに記憶しており、これによって各プライベートホストPH1…のPAをアドレス変換装置AD”のGAに多対一にマップすることを可能としている。具体的には、アドレス変換装置AD”がプライベートネットワークPNから受信したパケットを図12に示すフローチャートに従って処理するとともに、インターネットINから受信したパケットを図13に示すフローチャートに従って処理する。

【0009】図12に示すようにアドレス変換装置AD”は、任意のプライベートホストPH1…から受信したパケットから送信元のIPアドレスとポート番号PPとを読み出す（Step1）。そして、読み出したPAとPPの対（PA, PP）に対応するGPが内部テーブルに記憶されているか否かを判断し（Step2）、記憶されている場合にはパケット内のPAを格納する各フィールドにGAを書き込む（Step3）とともにパケット内のPPを格納する各フィールドにGPを書き込むことにより（Step4）、グローバルIPアドレスが付与されていないプライベートホストPH1…からのパケットの送信元アドレスをGAに変換するとともに送信元のポート番号PPをユニークなポート番号GPに変換する。そして、アドレス変換されたパケットをインターネットINに転送する（Step5）。

【0010】また（PA, PP）に対応するGPが内部テーブルに記憶されていない場合には、その（PA, PP）に対してユニークなGPが生成できるか否かを判断し（Step6）、生成できなければパケットを廃棄し（Step12）、生成できる場合には（PA, PP）に対応した

ユニークなGPを作成して(Step7)、内部テーブルに(PA, PP)と生成したGPを格納するエントリを付け加える(Step8)。そして、パケット内のPAを格納する各フィールドにGAを書き込む(Step9)とともにパケット内のPPを格納する各フィールドにGPを書き込むことにより(Step10)、グローバルIPアドレスが付与されていないプライベートホストPH1…からのパケットの送信元アドレスをGAに変換するとともに送信元のポート番号PPをユニークなポート番号GPに変換する。そして、アドレス変換されたパケットをインターネットINに転送する(Step11)。

【0011】一方、アドレス変換装置AD”がインターネットINの任意のインターネットホストIH1…からのパケットを受信すると、図13に示すようにパケットからGPを読み出し(Step1)、内部テーブルにそのGPに対応する(PA, PP)の対が有るか否かを判断する(Step2)。そして、対応する(PA, PP)の対が内部テーブルに有る場合には、パケット内のGAを格納する各フィールドにそのPAを書き込むとともに(Step3)、パケット内のGPを格納する各フィールドにPPを書き込むことにより(Step4)、送信先のアドレスをアドレス変換装置AD”のGAから何れかのプライベートホストPH1…のプライベートIPアドレスPAに変換するアドレス変換を行う。そして、アドレス変換されたパケットをプライベートネットワークPNに送る(Step5)。なお、内部テーブルに受信パケットのGPと対応する(PA, PP)の対がない場合にはそのパケットが廃棄される(Step6)。

【0012】

【発明が解決しようとする課題】ところが上記2つのネットワークアドレス変換方法でプライベートネットワークPNとインターネットINとを接続しているアドレス変換装置AD”において、TCP/IPの上位プロトコル(アプリケーション)毎に対応した処理が必要になる。これがシステムの複雑さを増し、性能を低下させる。特にIPマスカレードにおいては、IPアドレスだけでなくポート番号も変換するので、対応するアプリケーションの数が増え、さらに処理の複雑さが増し、性能が低下することになる。

【0013】本発明は上記事情に鑑みて為されたものであり、その目的とするところは、ポート番号を変換せずにプライベートなネットワークを構成する複数の端末間でグローバルなIPアドレスを同時に共有することが可能なネットワークアドレス変換方法及びその装置を提供することにある。

【0014】

【課題を解決するための手段】請求項1の発明は、上記目的を達成するために、インターネットプロトコルにおけるプライベートなIPアドレスが付与された複数の端末から構成されるプライベートネットワークをインターネットに接続し、パケット毎にプライベートなIPアドレスと前記プライベートネットワークに付与されたグローバルなIPアド

ネットに接続し、パケット毎にプライベートなIPアドレスと前記プライベートネットワークに付与されたグローバルなIPアドレスとのアドレス変換を行うアドレス変換手段によって前記各端末からインターネットへのパケットの送受信を可能とするネットワークアドレス変換方法において、前記アドレス変換手段にて前記各端末で一連のトランザクション処理に付与されたポート番号とパケットの送信先のグローバルなIPアドレスとの対を各端末のプライベートなIPアドレスに適宜対応付けることによってプライベートなIPアドレスとグローバルなIPアドレスとのアドレス変換を行うことを特徴とし、ポート番号を変換せずにプライベートなネットワークを構成する複数の端末間でグローバルなIPアドレスを同時に共有することが可能となり、その結果、未知の上位プロトコルの通信を破壊するようなことを最小限に抑えることができるとともに、アドレス変換の前後で送信元のポート番号が変化しないためにシステムの複雑さを減らし、且つ性能を向上させることができる。

【0015】請求項2の発明は、請求項1の発明において、前記アドレス変換手段が備える内部テーブルに各端末での一連のトランザクション処理に付与されたポート番号及び送信先のグローバルなIPアドレスの対とプライベートなIPアドレスとの対応関係を記憶させ、プライベートネットワークから受信したパケットの送信元のポート番号及び送信先のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には前記内部テーブルに当該対と送信元のプライベートなIPアドレスとの対応関係を記憶するとともにパケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、一致する場合には当該パケットの送信元のアドレスを前記内部テーブルの一一致した対応関係のプライベートなIPアドレスと比較して一致しない場合には当該パケットを廃棄するとともに一致する場合には当該パケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、インターネットから受信したパケットの送信先のポート番号及び送信元のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には当該パケットを廃棄するとともに、一致する場合には前記対応関係に基づいて当該パケットの送信先のアドレスをプライベートなIPアドレスに置き換えることを特徴とし、請求項1の発明の望ましい実施態様である。

【0016】請求項3の発明は、上記目的を達成するために、インターネットプロトコルにおけるプライベートなIPアドレスが付与された複数の端末から構成されるプライベートネットワークをインターネットに接続し、パケット毎にプライベートなIPアドレスと前記プライベートネットワークに付与されたグローバルなIPアド

レスとのアドレス変換を行って前記各端末からインターネットへのパケットの送受信を可能とするネットワークアドレス変換装置において、前記各端末で一連のトランザクション処理に付与されたポート番号とパケットの送信先のグローバルなIPアドレスとの対を各端末のプライベートなIPアドレスに適宜対応付けることによってプライベートなIPアドレスとグローバルなIPアドレスとのアドレス変換を行うアドレス変換手段を備えたことを特徴とし、ポート番号を変換せずにプライベートなネットワークを構成する複数の端末間でグローバルなIPアドレスを同時に共有することが可能となり、その結果、未知の上位プロトコルの通信を破壊するようなことを最小限に抑えることができるとともに、アドレス変換の前後で送信元のポート番号が変化しないためにシステムの複雑さを減らし、且つ性能を向上させることができる。

【0017】請求項4の発明は、請求項3の発明において、前記アドレス変換手段に各端末での一連のトランザクション処理に付与されたポート番号及び送信先のグローバルなIPアドレスの対とプライベートなIPアドレスとの対応関係を記憶する内部テーブルを備え、プライベートネットワークから受信したパケットの送信元のポート番号及び送信先のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には前記内部テーブルに当該対と送信元のプライベートなIPアドレスとの対応関係を記憶するとともにパケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、一致する場合には当該パケットの送信元のプライベートなIPアドレスを前記内部テーブルの一致した対応関係のプライベートなIPアドレスと比較して一致しない場合には当該パケットを廃棄するとともに一致する場合には当該パケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、インターネットから受信したパケットの送信先のポート番号及び送信元のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には当該パケットを廃棄するとともに、一致する場合には前記対応関係に基づいて当該パケットの送信先のアドレスをプライベートなIPアドレスに置き換えることを特徴とし、請求項3の発明の望ましい実施態様である。

【0018】請求項5の発明は、請求項3又は4の発明において、インターネットプロトコルにおけるルーティングやフィルタリングを行うルータの機能を備えたことを特徴とし、ルータが別途不要となって設備の削減が図れるという利点がある。

【0019】

【発明の実施の形態】図1～図8を参照して本発明を実施形態により詳細に説明する。

【0020】図2は本実施形態におけるプライベートネットワークPNの構成例を示しており、複数台（例えば5台）の端末、例えばプライベートホストPH1～PH5がIPルータを兼ねるアドレス変換装置ADにバス接続されてLAN（イーサネット）が構築されている。

【0021】プライベートネットワーク内の各プライベートホストPH1～PH5並びにアドレス変換装置ADには、プライベートネットワーク内でのみ有効であってインターネットINでは有効でないプライベートIPアドレス[10.0.0.1]、[10.0.0.2]、[10.0.0.3]、[10.0.0.4]、[10.0.0.5]、[10.0.0.19]がそれぞれ付与されている。また、アドレス変換装置ADにはインターネットINで有効なグローバルIPアドレス[133.0.0.2]が付与されている。

【0022】図1に示すように、アドレス変換装置ADはOSI参照モデルにおける物理層及びデータリンク層に相当するハードウェア1と、IPアドレスに基づいてパケットのルーティングやフィルタリングあるいは中継処理などを行い、OSI参照モデルにおけるネットワーク層に相当するIPレヤー2と、本発明の要旨であり、プライベートIPアドレスをアドレス変換装置ADに付与されたグローバルIPアドレスにアドレス変換するアドレス変換レヤー3とを備えている。そして、アドレス変換レヤー3においては、プライベートネットワークPNのプライベートホストPH1…から受信したパケットPを図6に示すフローチャートに従って処理するとともに、インターネットINのインターネットホストIH1…から受信したパケットPを図7に示すフローチャートに従って処理する。なお、本実施形態ではプライベートネットワークPNの各プライベートホストPH1～PH5とインターネットINの任意のインターネットホストIH1…との間の通信プロトコルにOSI参照モデルのトランスポート層に対応するTCPを用いる場合について説明するが、TCPの代わりにUDPを用いることも可能である。

【0023】以下、図3に示すようにアドレス変換装置ADを介してプライベートホストPH1～PH5とインターネットホストIH1～IH4との間で6通りのTCPコネクション1～6を設立する場合を例にして、アドレス変換レヤー3でのアドレス変換手順を説明する。同図において、点線矢印はTCPコネクション1～6をそれぞれ表しており、矢印の起点がコネクションの設立を要求するホストであり、矢印の先がコネクション設立要求相手のホストである。また、図4及び図5は上記TCPコネクション1～6の設立要求パケットや設立確認パケット並びに情報パケットとアドレス変換装置ADでパケットを送受信したときの内部テーブルTaの内容などを時間的な流れに沿って表した模式図である。

【0024】ここで、アドレス変換装置ADの内部テーブルTaには、パケットを送信したプライベートホスト

P H 1 …にて一連のトランザクション処理に付与された送信元（ソース）のポート番号（以下、「S P」と表記）と、送信先（デスティネーション）のインターネットホスト I H 1 …のグローバル I P アドレス（以下、「I A」と表記）との対を、送信元のプライベート I P アドレス P A に対応付けた対応関係が記憶されている。いま、内部テーブル T a の初期状態では、図 4 に示すようにプライベートホスト P H 3 のプライベート I P アドレス P A (= [10.0.0.3]) と、送信元のポート番号 S P (= [21]) 及び任意のインターネットホスト I H 1 …の I P アドレス I A (" * " で表す) の対とが対応付けられて記憶されているものとする。但し、これは一例であって、必ずしも初期状態で内部テーブル T a に何らかの対応関係が記憶されている必要はない。

【0025】図 4 に示すようにプライベートホスト P H 1 がインターネットホスト I H 1 に対して送信した T C P コネクション 1 の設立要求のパケット P 1 が最初にアドレス変換装置 A D に受信されると、パケット P 1 の送信元の I P アドレス（プライベートホスト P H 1 のプライベート I P アドレス P A = [10.0.0.1]）、送信元のポート番号（プライベートホスト P H 1 のポート番号 P P = [2565]）、送信先の I P アドレス（インターネットホスト I H 1 のグローバル I P アドレス I A = [129.15.10.1.17]）を読み出し（図 6 の Step 1）、内部テーブル T a にこの（P P, I A）の対に対応する P A が記憶されているか否かを判断する（図 6 の Step 2）。今の場合には内部テーブル T a が初期状態であるから上記（P P, I A）の対に対応する P A は記憶されていないため、内部テーブル T a に上記（P P, I A）の対と P A を格納するエントリを付け加え（図 6 の Step 7）、パケット P 1 内の P A を格納するフィールドにグローバル I P アドレス G A (= [133.0.0.2]) を書き込むことで送信元アドレスの変換を行ない（図 6 の Step 8）、変換後のパケット P 1' をインターネット I N に転送する（図 6 の Step 9）。このパケット P 1' は、送信元の I P アドレスがアドレス変換装置 A D に付与されたグローバル I P アドレス G A に変換されているためにインターネットホスト I H 1 にて受信される。

【0026】次にプライベートホスト P H 2 がインターネットホスト I H 1 に対して送信した T C P コネクション 2 の設立要求のパケット P 2 がアドレス変換装置 A D に受信されると、パケット P 2 の送信元の I P アドレス（プライベートホスト P H 2 のプライベート I P アドレス P A = [10.0.0.2]）、送信元のポート番号（プライベートホスト P H 2 のポート番号 P P = [4039]）、送信先の I P アドレス（インターネットホスト I H 1 のグローバル I P アドレス I A = [129.15.101.17]）を読み出し（図 6 の Step 1）、内部テーブル T a にこの（P P, I A）の対に対応する P A が記憶されているか否かを判断する（図 6 の Step 2）。今の場合には内部テーブル T a

には上記（P P, I A）の対に対応する P A は記憶されていないため、内部テーブル T a に上記（P P, I A）の対と P A を格納するエントリを付け加え（図 6 の Step 7）、パケット P 2 内の P A を格納するフィールドにグローバル I P アドレス G A (= [133.0.0.2]) を書き込むことで送信元アドレスの変換を行ない（図 6 の Step 8）、変換後のパケット P 2' をインターネット I N に転送する（図 6 の Step 9）。このパケット P 2' もまた送信元の I P アドレスがアドレス変換装置 A D に付与されたグローバル I P アドレス G A に変換されているためにインターネットホスト I H 1 にて受信される。

【0027】次にインターネットホスト I H 2 が送信した T C P コネクション 3 の設立要求のパケット P 3 がアドレス変換装置 A D に受信されると、パケット P 3 の送信先のポート番号（アドレス変換装置 A D のポート番号 G P = [21]）と送信元の I P アドレス（インターネットホスト I H 2 のグローバル I P アドレス I A = [133.254.180.17]）を読み出し（図 7 の Step 1）、内部テーブル T a にこの（G P, I A）の対に対応する P A が記憶されているか否かを判断する（図 7 の Step 2）。今の場合には内部テーブル T a の初期値として上記（G P, I A）の対に対応する P A（プライベートホスト P H 3 のプライベート I P アドレス P A = [10.0.0.3]）が記憶されているため、パケット P 3 内の G A を格納するフィールドに上記プライベートホスト P H 3 のプライベート I P アドレス P A を書き込むことで送信先アドレスの変換を行ない（図 7 の Step 3）、変換後のパケット P 3' をプライベートネットワーク P N に転送する（図 7 の Step 4）。そして、このパケット P 3' は、送信先の I P アドレスがプライベートホスト P H 3 のプライベート I P アドレス P S に変換されているためにプライベートホスト P H 3 にて受信される。

【0028】次にインターネットホスト I H 3 が送信した T C P コネクション 4 の設立要求のパケット P 4 がアドレス変換装置 A D に受信されると、パケット P 4 の送信先のポート番号（アドレス変換装置 A D のポート番号 G P = [1500]）と送信元の I P アドレス（インターネットホスト I H 3 のグローバル I P アドレス I A = [130.69.245.44]）を読み出し（図 7 の Step 1）、内部テーブル T a にこの（G P, I A）の対に対応する P A が記憶されているか否かを判断する（図 7 の Step 2）。今の場合には内部テーブル T a に上記（G P, I A）の対に対応する P A が記憶されていないため、このパケット P 4 を廃棄する（図 7 の Step 5）。従って、インターネットホスト I H 3 からのコネクション設立要求に対しては T C P コネクションが設立されない。

【0029】次にプライベートホスト P H 4 がインターネットホスト I H 4 に対して送信した T C P コネクション 5 の設立要求のパケット P 5 がアドレス変換装置 A D に受信されると、パケット P 5 の送信元の I P アドレス

(プライベートホストPH4のプライベートIPアドレスPA=[10.0.0.4])、送信元のポート番号(プライベートホストPH4のポート番号PP=[5005])、送信先のIPアドレス(インターネットホストIH4のグローバルIPアドレスIA=[128.250.0.120])を読み出し(図6のStep1)、内部テーブルTaにこの(PP, IA)の対に対応するPAが記憶されているか否かを判断する(図6のStep2)。今の場合には内部テーブルTaには上記(PP, IA)の対に対応するPAは記憶されていないため、内部テーブルTaに上記(PP, IA)の対とPAを格納するエントリを付け加え(図6のStep7)、パケットP5内のPAを格納するフィールドにグローバルIPアドレスGA(=[133.0.0.2])を書き込むことで送信元アドレスの変換を行ない(図6のStep8)、変換後のパケットP5'をインターネットINに転送する(図6のStep9)。このパケットP5'もまた送信元のIPアドレスがアドレス変換装置ADに付与されたグローバルIPアドレスGAに変換されているためにインターネットホストIH4にて受信される。

【0030】次にプライベートホストPH5がインターネットホストIH4に対して送信したTCPコネクション6の設立要求のパケットP6がアドレス変換装置ADに受信されると、パケットP6の送信元のIPアドレス(プライベートホストPH5のプライベートIPアドレスPA=[10.0.0.5])、送信元のポート番号(プライベートホストPH5のポート番号PP=[5005])、送信先のIPアドレス(インターネットホストIH4のグローバルIPアドレスIA=[128.250.0.120])を読み出し(図6のStep1)、内部テーブルTaにこの(PP, IA)の対に対応するPAが記憶されているか否かを判断する(図6のStep2)。ここで、内部テーブルTaには上記(PP, IA)の対に対応する別のPA(プライベートホストPH4のプライベートIPアドレス)が既に記憶されているため、このパケットP6を廃棄する(図6のStep6)。

【0031】ところで、図5に示すようにプライベートホストPH1からのTCPコネクション1の設立要求パケットP1'を受信したインターネットホストIH1は、TCPコネクション1の設立要求パケットP1'の送信元のIPアドレス及びポート番号をそれぞれ送信先のIPアドレス及びポート番号としたTCPコネクション1の設立確認のパケットP7を送信する。そして、この設立確認のパケットP7を受信したアドレス変換装置ADでは、パケットP7の送信先のポート番号(アドレス変換装置ADのポート番号GP=[2565])と送信元のIPアドレス(インターネットホストIH1のグローバルIPアドレスIA=[129.15.101.17])を読み出し(図7のStep1)、内部テーブルTaにこの(GP, IA)の対に対応するPAが記憶されているか否かを判断する(図7のStep2)。今の場合には内部テーブルTa

に上記(GP, IA)の対に対応するPA(プライベートホストPH1のプライベートIPアドレスPA=[10.0.0.1])が記憶されているため、パケットP7内のGAを格納するフィールドに上記プライベートホストPH1のプライベートIPアドレスPAを書き込むことで送信先アドレスの変換を行ない(図7のStep3)、変換後のパケットP7'をプライベートネットワークPNに転送する(図7のStep4)。そして、このパケットP7'は、送信先のIPアドレスがプライベートホストPH1のプライベートIPアドレスPAに変換されているためにプライベートホストPH1にて受信される。その結果、プライベートホストPH1とインターネットホストIH1との間でTCPコネクション1が設立される。

【0032】続いて、プライベートホストPH1からは設立されたTCPコネクション1を使って情報パケットP8を送信する。アドレス変換装置ADではこのパケットP8を受信すると、パケットP8の送信元のIPアドレス(プライベートホストPH1のプライベートIPアドレスPA=[10.0.0.1])、送信元のポート番号(プライベートホストPH1のポート番号PP=[2565])、送信先のIPアドレス(インターネットホストIH1のグローバルIPアドレスIA=[129.15.101.17])を読み出し(図6のStep1)、内部テーブルTaにこの(PP, IA)の対に対応するPAが記憶されているか否かを判断する(図6のStep2)。今の場合には内部テーブルTaには上記(PP, IA)の対に対応するPAが記憶されているから、パケットP8内のPAを格納するフィールドにグローバルIPアドレスGA(=[133.0.0.2])を書き込むことで送信元アドレスの変換を行ない(図6のStep8)、変換後のパケットP8'をインターネットINに転送する(図6のStep9)。このパケットP8'もまた送信元のIPアドレスがアドレス変換装置ADに付与されたグローバルIPアドレスGAに変換されているためにインターネットホストIH1にて受信される。

【0033】上述のように本発明のアドレス変換方法並びにアドレス変換装置ADにおいては、プライベートホストPH1…のポート番号PP及び当該プライベートホストPH1…からのパケットの送信先に指定されたインターネットホストIH1…のグローバルIPアドレスIAの対(PP, IA)と、当該プライベートホストPH1…のプライベートIPアドレスPAとの対応関係を内部テーブルTaに記憶し、この対応関係に基づいて、アドレス変換装置ADに付与されている1つのグローバルIPアドレスGPを複数台のプライベートホストPH1…のプライベートIPアドレスPAに1対多にマップすることができ、しかもプライベートホストPH1…のポート番号PPと、アドレス変換装置ADとインターネットホストIH1…との間で送受信されるパケットのポート番号GPとがNATと同様に常に一致しているため、

未知の上位プロトコルの通信を破壊するようなことを最小限に抑えることができるとともに、NATと同様にアドレス変換の前後で送信元のポート番号SPが変化しないため、IPマスクレードに比較してシステムの複雑さを減らし、且つ性能を向上させることができるとなる。

【0034】なお、本実施形態ではアドレス変換装置ADがIPルータの機能を兼ね備えるようにしているが、必ずしもIPルータの機能を兼ね備える必要はなく、図8に示すようにアドレス変換装置AD'がハードウェア1とアドレス変換レヤー3を備え、IPルータRを別途外部に接続する構成としてもよい。このような構成とすれば、IPルータRを備えた既存のネットワークに本発明のアドレス変換装置AD'を導入する場合でもIPルータRがそのまま使用できるという利点がある。

【0035】

【発明の効果】請求項1の発明は、インターネットプロトコルにおけるプライベートなIPアドレスが付与された複数の端末から構成されるプライベートネットワークをインターネットに接続し、パケット毎にプライベートなIPアドレスと前記プライベートネットワークに付与されたグローバルなIPアドレスとのアドレス変換を行うアドレス変換手段によって前記各端末からインターネットへのパケットの送受信を可能とするネットワークアドレス変換方法において、前記アドレス変換手段にて前記各端末で一連のトランザクション処理に付与されたポート番号とパケットの送信先のグローバルなIPアドレスとの対を各端末のプライベートなIPアドレスに適宜対応付けることによってプライベートなIPアドレスとグローバルなIPアドレスとのアドレス変換を行うので、ポート番号を変換せずにプライベートなネットワークを構成する複数の端末間でグローバルなIPアドレスを同時に共有することができる。その結果、未知の上位プロトコルの通信を破壊するようなことを最小限に抑えることができるとともに、アドレス変換の前後で送信元のポート番号が変化しないためにシステムの複雑さを減らし、且つ性能を向上させることができるという効果がある。

【0036】請求項2の発明は、前記アドレス変換手段が備える内部テーブルに各端末での一連のトランザクション処理に付与されたポート番号及び送信先のグローバルなIPアドレスの対とプライベートなIPアドレスとの対応関係を記憶させ、プライベートネットワークから受信したパケットの送信元のポート番号及び送信先のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には前記内部テーブルに当該対と送信元のプライベートなIPアドレスとの対応関係を記憶するとともにパケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、一致する場合には当該パケットの送信元のプライベートなIP

アドレスを前記内部テーブルの一一致した対応関係のプライベートなIPアドレスと比較して一致しない場合には当該パケットを廃棄するとともに一致する場合には当該パケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、インターネットから受信したパケットの送信先のポート番号及び送信元のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には当該パケットを廃棄するとともに、一致する場合には前記対応関係に基づいて当該パケットの送信先のアドレスをプライベートなIPアドレスに置き換えるので、請求項1の発明と同様の効果を奏すことができる。

【0037】請求項3の発明は、インターネットプロトコルにおけるプライベートなIPアドレスが付与された複数の端末から構成されるプライベートネットワークをインターネットに接続し、パケット毎にプライベートなIPアドレスと前記プライベートネットワークに付与されたグローバルなIPアドレスとのアドレス変換を行って前記各端末からインターネットへのパケットの送受信を可能とするネットワークアドレス変換装置において、前記各端末で一連のトランザクション処理に付与されたポート番号とパケットの送信先のグローバルなIPアドレスとの対を各端末のプライベートなIPアドレスに適宜対応付けることによってプライベートなIPアドレスとグローバルなIPアドレスとのアドレス変換を行うアドレス変換手段を備えたので、ポート番号を変換せずにプライベートなネットワークを構成する複数の端末間でグローバルなIPアドレスを同時に共有することができるとなり、その結果、未知の上位プロトコルの通信を破壊するようなことを最小限に抑えることができるとともに、アドレス変換の前後で送信元のポート番号が変化しないためにシステムの複雑さを減らし、且つ性能を向上させることができるという効果がある。

【0038】請求項4の発明は、前記アドレス変換手段に各端末での一連のトランザクション処理に付与されたポート番号及び送信先のグローバルなIPアドレスの対とプライベートなIPアドレスとの対応関係を記憶する内部テーブルを備え、プライベートネットワークから受信したパケットの送信元のポート番号及び送信先のグローバルなIPアドレスの対を前記内部テーブルに記憶されている対応関係と比較し、一致しない場合には前記内部テーブルに当該対と送信元のプライベートなIPアドレスとの対応関係を記憶するとともにパケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換え、一致する場合には当該パケットの送信元のプライベートなIPアドレスを前記内部テーブルの一一致した対応関係のプライベートなIPアドレスと比較して一致しない場合には当該パケットを廃棄するとともに一致する場合には当該パ

ケットの送信元のアドレスを前記プライベートネットワークに付与されているグローバルなIPアドレスに置き換える、インターネットから受信したパケットの送信先のポート番号及び送信元のグローバルなIPアドレスの対を前記内部テーブルに記憶している対応関係と比較し、一致しない場合には当該パケットを廃棄するとともに、一致する場合には前記対応関係に基づいて当該パケットの送信先のアドレスをプライベートなIPアドレスに置き換えるので、請求項3の発明と同様の効果を奏すことができる。

【0039】請求項5の発明は、インターネットプロトコルにおけるルーティングやフィルタリングを行うルータの機能を備えたので、IPルータを備えた既存のネットワークにアドレス変換装置を導入する場合でもIPルータがそのまま使用できるという効果がある。

【図面の簡単な説明】

【図1】実施形態の概略構成図である。

【図2】同上を用いたネットワークの構成例を示す図である。

【図3】同上の動作説明図である。

【図4】同上の動作説明図である。

【図5】同上の動作説明図である。

【図6】同上におけるプライベートネットワークからインターネットへのパケットの処理を説明するためのフローチャートである。

10

【図7】同上におけるインターネットからプライベートネットワークへのパケットの処理を説明するためのフローチャートである。

【図8】同上の他の例を示す概略構成図である。

【図9】従来のネットワーク構成例を示す図である。

【図10】従来のNATによるプライベートネットワークからインターネットへのパケットの処理を説明するためのフローチャートである。

【図11】従来のNATによるインターネットからプライベートネットワークへのパケットの処理を説明するためのフローチャートである。

【図12】従来のIPマスカレードによるプライベートネットワークからインターネットへのパケットの処理を説明するためのフローチャートである。

【図13】従来のIPマスカレードによるインターネットからプライベートネットワークへのパケットの処理を説明するためのフローチャートである。

【符号の説明】

AD アドレス変換装置

1 ハードウェア

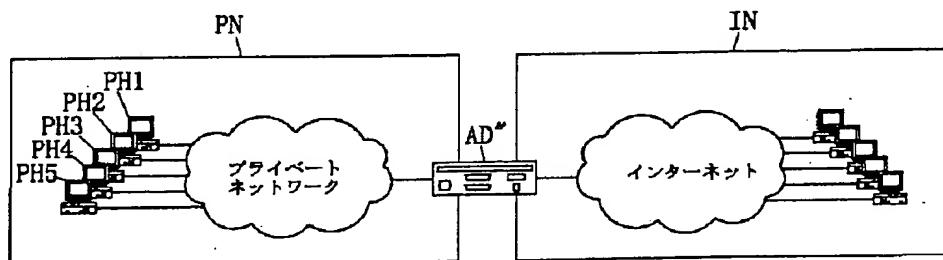
2 IPレヤー

3 アドレス変換レヤー

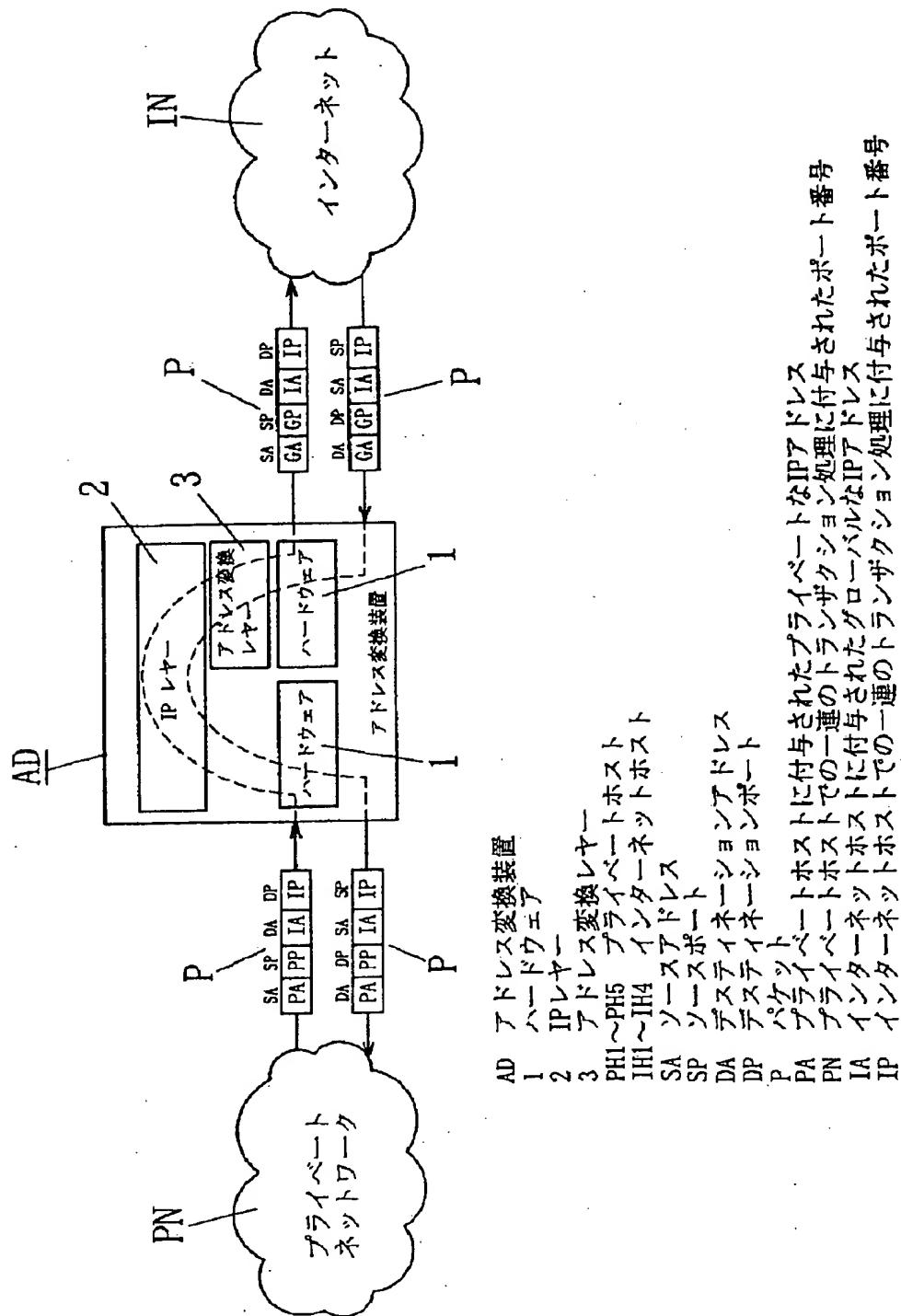
PH1～PH5 プライベートホスト

IH1～IH4 インターネットホスト

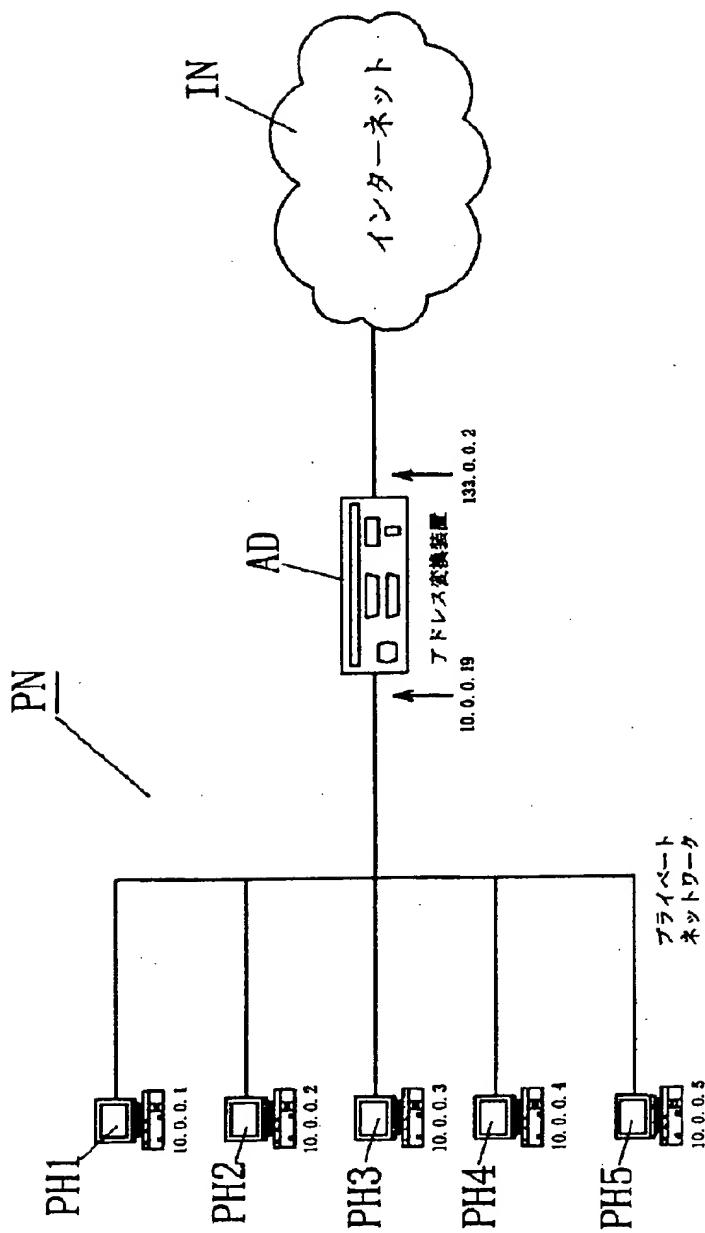
【図9】



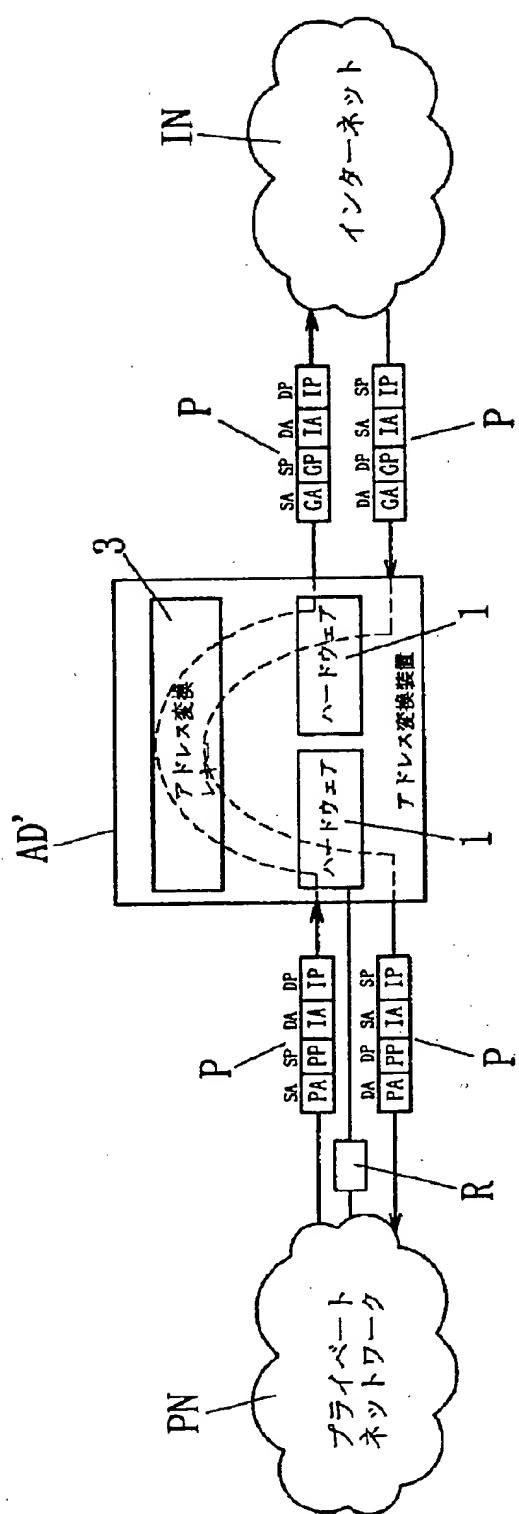
【図1】



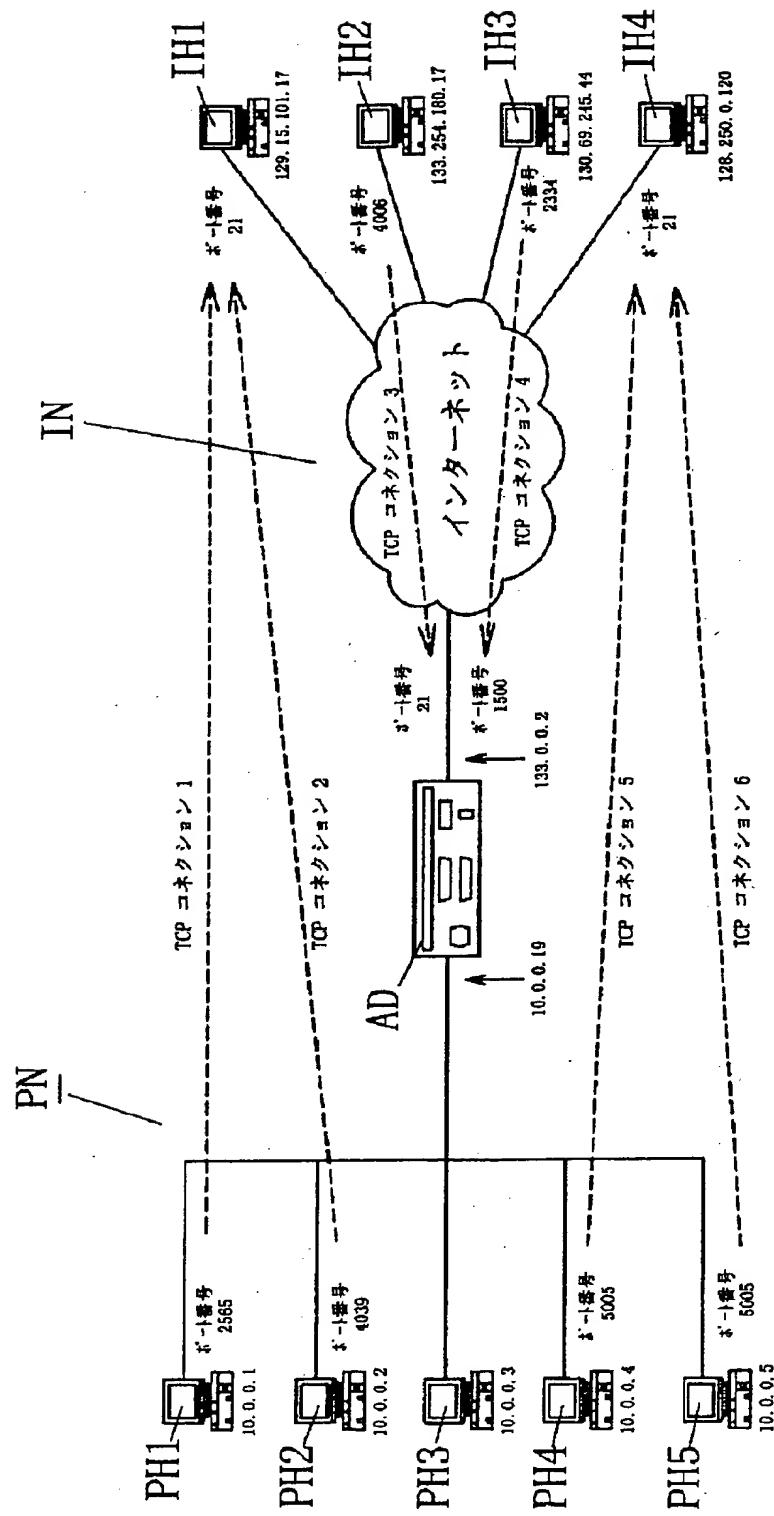
[図2]



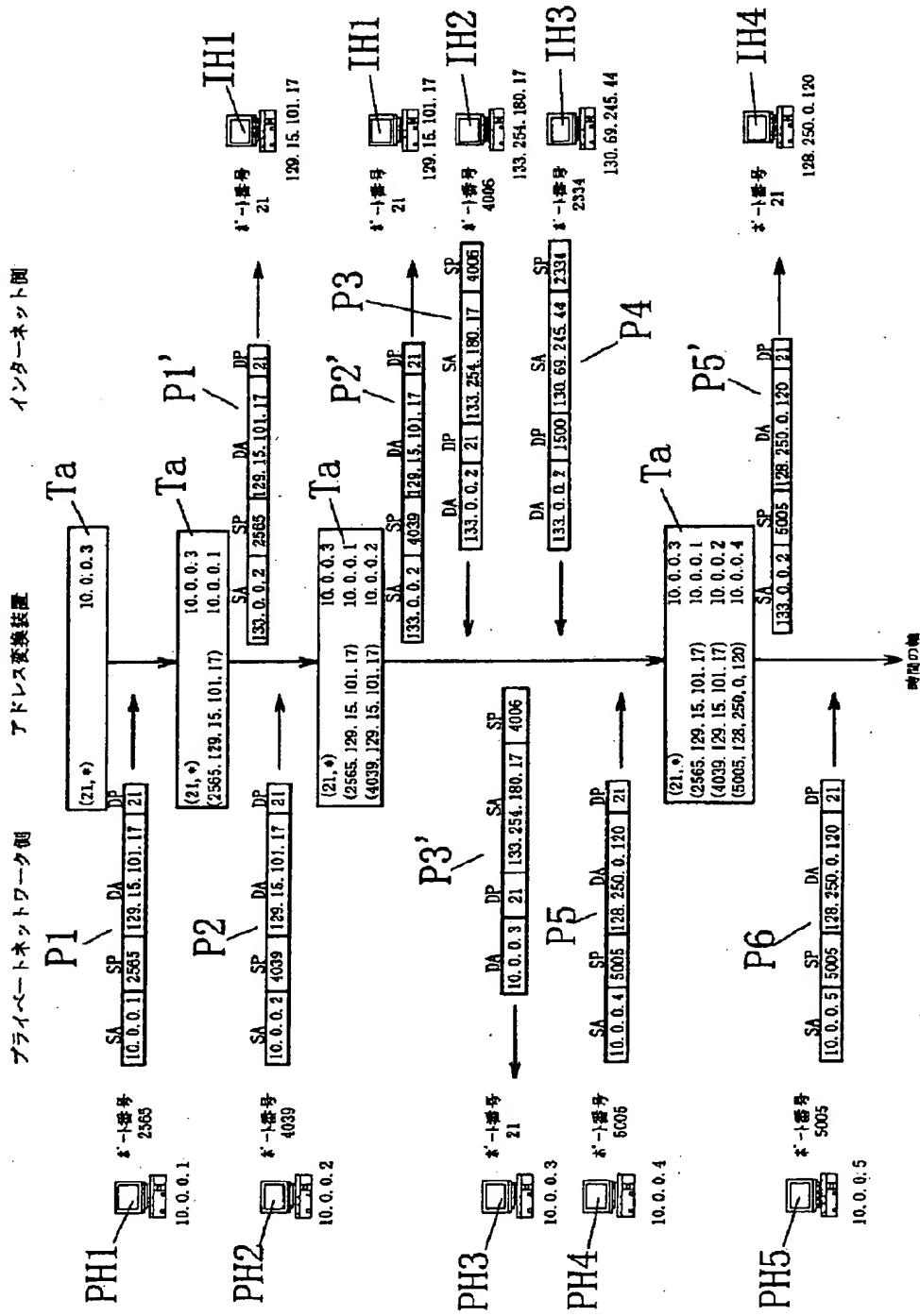
[図8]



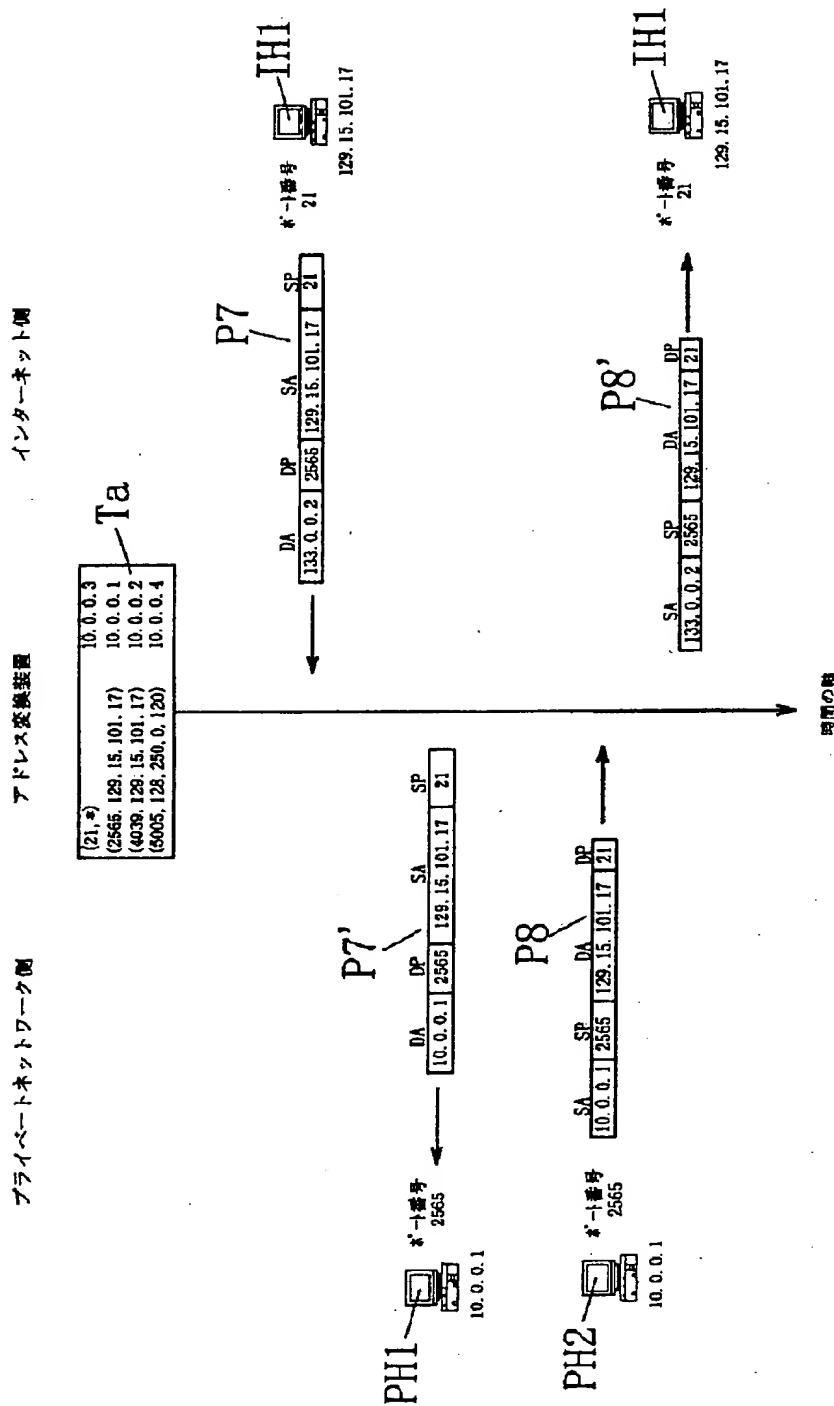
【図3】



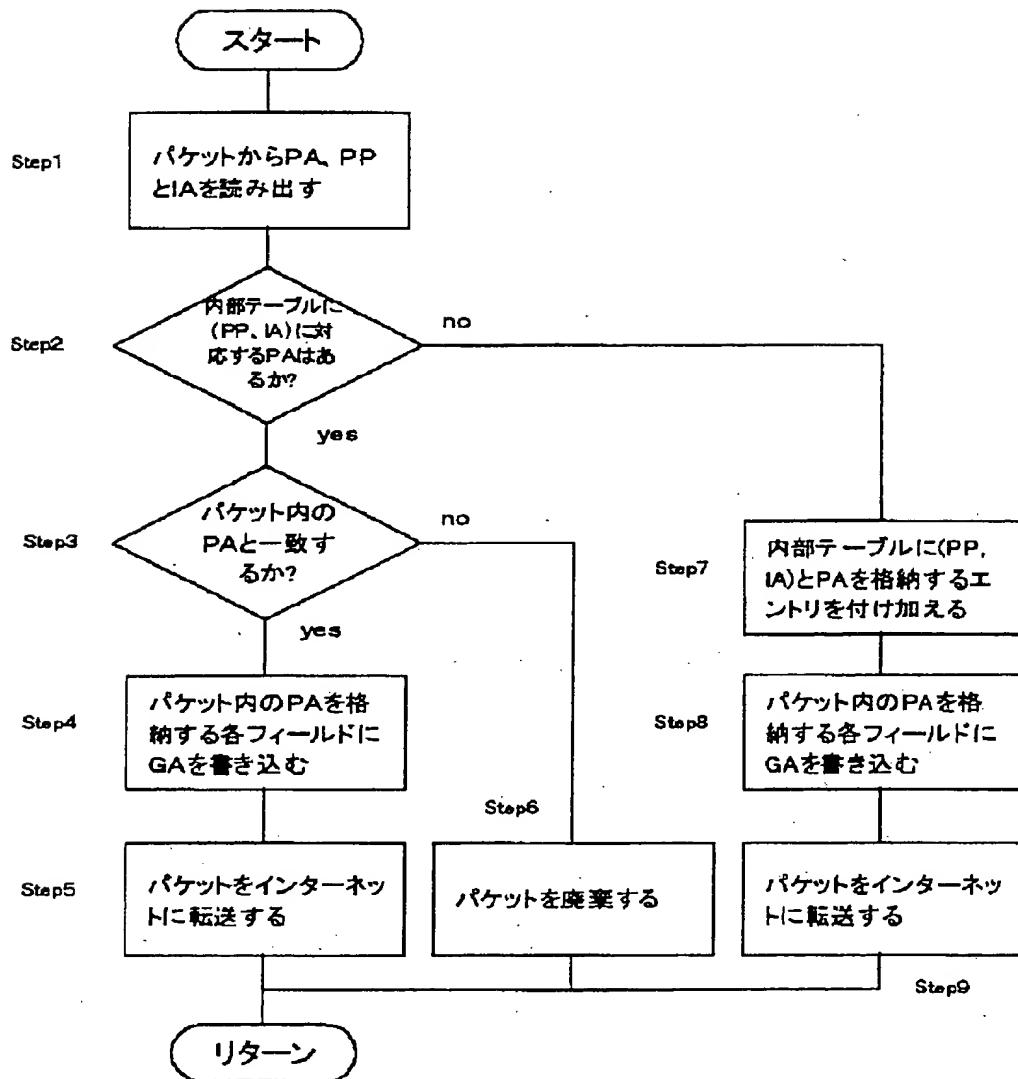
[図4]



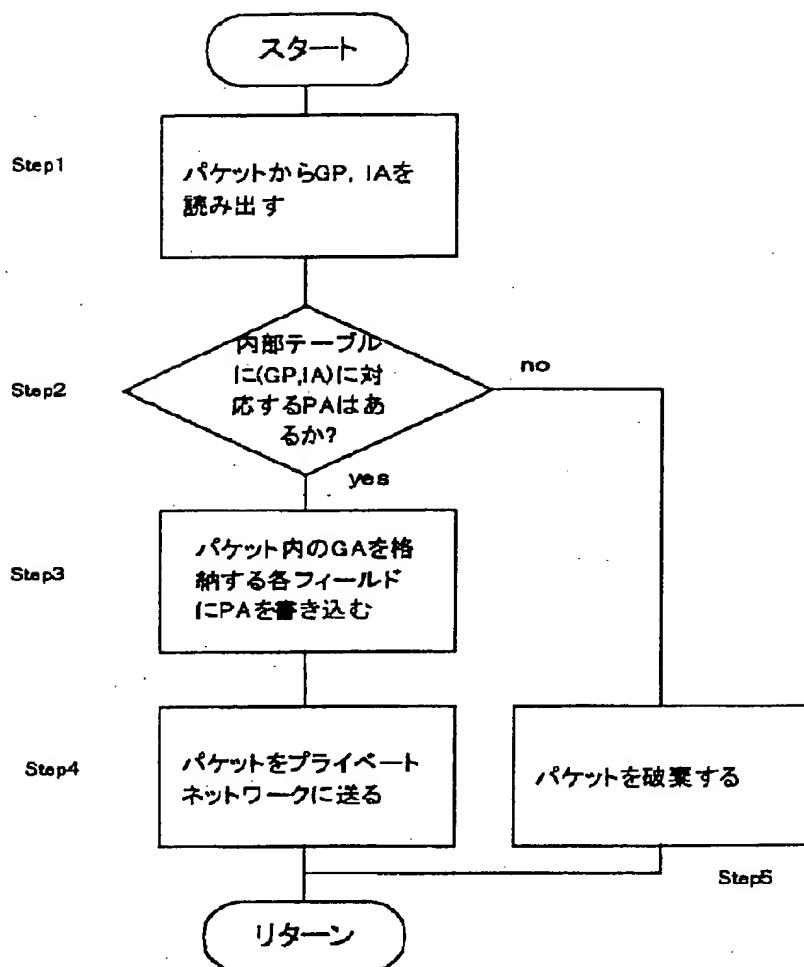
[図5]



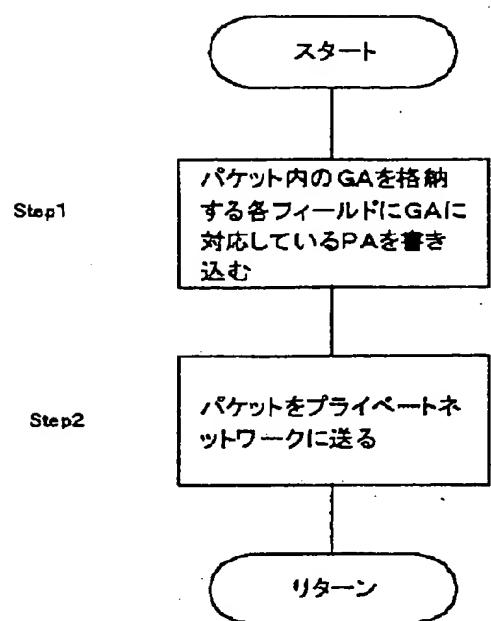
【図6】



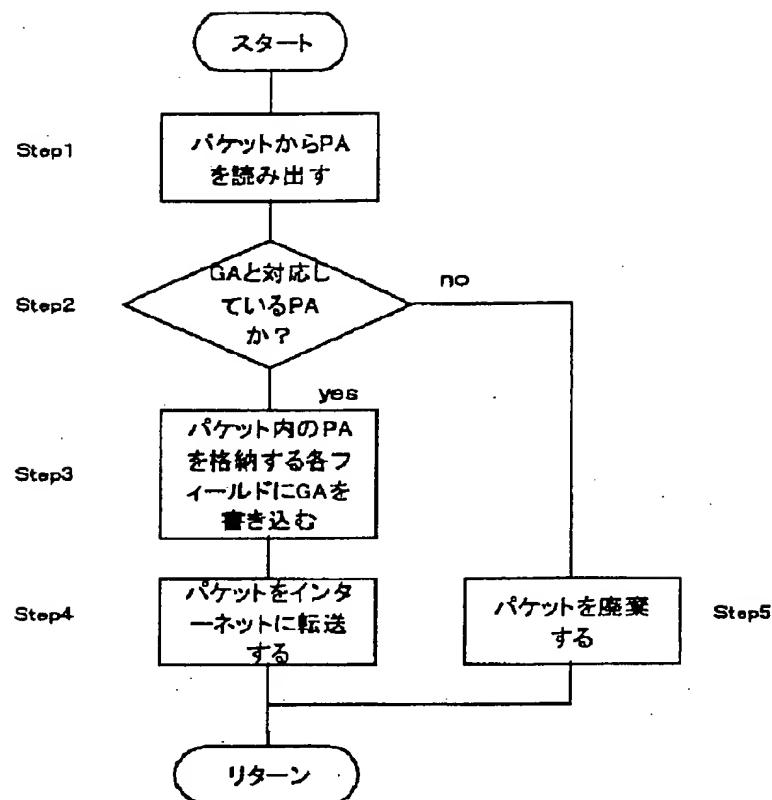
【図7】



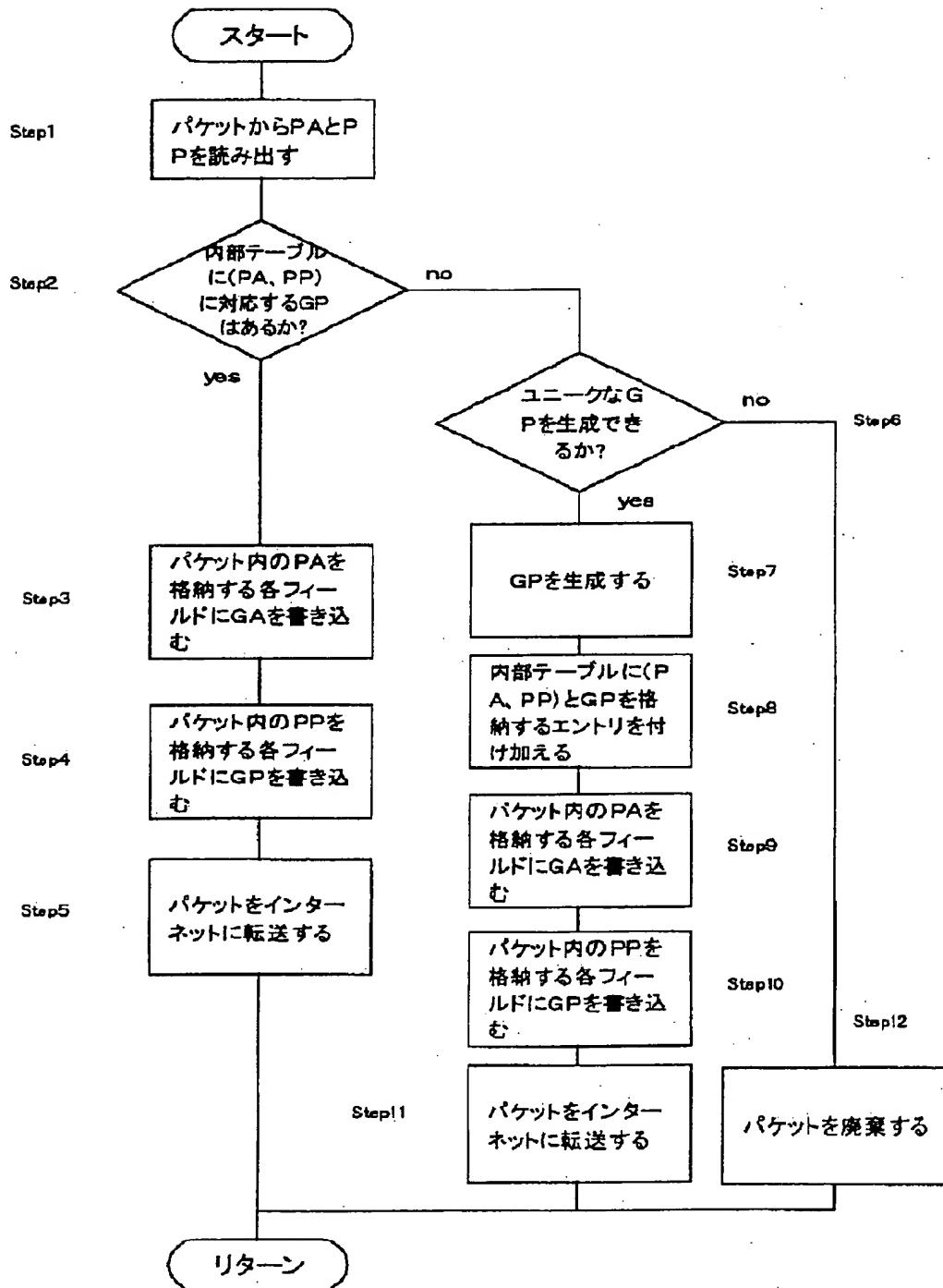
【図11】



【図10】



【図12】



【図13】

